ISSUE PAPER

SCOPE OF DCID 1/16

ISSUE:

Should the revision of DCID 1/16 modify the scope of the information protected as cited in the current DCID 1/16?

PROBLEM:

To select the scope for the rewrite of DCID 1/16.

ALTERNATIVES:

A. Retain the current DCID's scope; i.e., all "intelligence information."

B. Limit the DCID to SCI.

C. Expand the scope of the DCID to, specifically, include other information, such as tactical intelligence.

BACKGROUND:

The scope of the current DCID 1/16 is defined by the following statements:

"Pursuant to the provisions of Section 102 of the National Security Act of 1947 and Executive Order 12333, policies and procedures are herewith established for the security of classified intelligence information (hereafter referred to as intelligence)* processed and stored in automated systems and networks.

---

*For purposes of this policy statement, classified intelligence information ("intelligence") means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources or methods, that has been classified pursuant to Executive Order 12356 (or successor order). "Foreign intelligence" and "counterintelligence" have the meanings assigned to them in Executive Order 12333. "Intelligence", as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982 (or successor manual)."

The existing statement of the scope of DCID 1/16 includes sensitive compartmented information (SCI) and information that is derived from sensitive intelligence sources or methods. The definitions referenced (but not directly quoted) in the existing DCID include the following*:

Foreign Intelligence - Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons.

Counterintelligence - Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, assassinations, or international terrorist activities.

Sensitive Compartmented Information (SCI)

- Information requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products.
- These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs.
- Does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

---

*Per E.O. 12333, E.O. 12356, and DCID 1/19-"DCI Security Policy Manual for SCI Control Systems", dated 28 June 1982

UNCLASSIFIED

ADVANTAGES AND DISADVANTAGES:

The advantages of retaining the current scope include the following:

A. The DCI's responsibilities are adequately referenced

B. No compelling reason for modification of the scope of the DCID

C. Although the scope has been misinterpreted by some components, it has proven usable over the life of the DCID.

Some components have indicated that the existing DCID refers ONLY to systems and networks processing SCI. The existing DCID clearly refutes this, both implicitly and explicitly. The advantages of the rewrite limiting itself to SCI are:

A. Such a document would be simpler, and much easier to implement.

B. The user community for such a document would be much smaller.

C. There would be absolutely no question of the applicability of the DCID.

The disadvantages of such a limit include the following:

A. The protection of information derived from sensitive intelligence sources or methods would be poorly-defined, and might revert to the protection appropriate for "plain-vanilla" classified material at the same level (i.e., some DCI defined protection mechanisms which are authorized by sections 1.3 (c) and 3.3 (c) of EO 12356 and promulgated in DCID 1/7 may not be implemented).

B. Protection of information under the DCI's purview would have been removed from his control.

Expanding the scope of the rewrite to explicitly cover some contentious areas, such as some tactical intelligence activities, is not recommended. The scope of the DCID already addresses these areas in the detail required by policy.

The DCID covers all "automated systems and networks" that process "intelligence information." There seems to be no rationale for narrowing this definition. However, there is reason for clarifying the (existing) scope. The language can be improved, without changing the meaning.

COMPARISON WITH OTHER POLICY STATEMENTS

A. DCID 1/16, dated 4 January 1983

The scope of the current DCID is identical to the suggested scope for the rewrite.

B. SAFEGUARDS dated December 1984

The scope of the SAFEGUARDS is the 13 "critical systems" specified by the DCI in his COMPUSEC project. Has been extended to a limited number of other systems based upon DDCI approval.

C. Proposed revision of DCID 1/16 developed by CSSS of SECOM in 1984

Suggested retaining the scope of the current DCID, but, explicitly including coverage of " . . . communications-related security, and to cover collateral intelligence information." As specified above, the current DCID covers collateral information, but, can be confusing. The specific inclusion of telecommunications would have been an expansion of the scope.

D. Redraft of CIA [redacted] (the red/white/blue book) STAT

"This document applies to all automated data processing systems owned or operated by the Agency or an Agency-contractor and all systems into which Agency-classified information is to be introduced, whether or not the Agency owns or operates such systems." DCID 1/16 is not in this document's list of references. STAT

Coverage appears to be overlapping, but, CIA [redacted] is the Agency's implementation of the COMPUSEC rules. No conflict is seen.

E. DoD Reg. 5200.28

Applies to all DoD (expanded) classified and sensitive unclassified computing.

Includes the statement: "Measures to protect foreign intelligence and foreign counterintelligence (e.g., sensitive compartmented information (SCI)) handled by an AIS shall meet the security requirements of this Directive and reference (e)." Reference (e) is DCID 1/16.

UNCLASSIFIED

F. DoD Reg. 5200.28-STD

Comparison is not applicable. DoD Reg. 5200.28-STD is a standard for evaluating ". . . [the] effectiveness of security controls built into automatic data processing products."

G. NSA Reg [ ] STAT

"This directive encompasses all ADP systems operated by NSA/CSS and its contractors. This includes all connections of NSA/CSS systems to other government computer systems and the provision of NSA system remote terminals to other government agencies." "These requirements apply to all NSA/CSS ADP systems and those of its affiliated contractors that are used to store, process or communicate classified and/or sensitive information. [emphasis added] DCID 1/16 is not in the list of references.

Possible conflicts are indeterminable at this time.

H. DoD 5030.58 (TELECOM manual)

"The purpose of this document is to provide DSSCS security criteria and telecommunications guidance for the protection of Sensitive Compartmented Information (SCI) stored and/or processed in a consolidated Defense Special Security Communications System/General Service (DSSCS/GENSER) Automated Message Processing System (AMPS). "The security criteria and guidance prescribed in this manual will be used in the system planning, equipment design, and determination of the security acceptability of an Automated Message Processing System (AMPS) to process and distribute SCI in unencrypted form."

I. DIAM 50-4 & 50-5 (Computer Security)

DIAM 50-4: "(U) PURPOSE: To implement the provisions of . . . DCID 1/16 . . . to provide policy guidance on the security requirements for the protection of . . . SCI stored and/or processed in and . . . an ADP system or netted ADP systems and to establish the criteria and procedures for the test, analysis, evaluation, and accreditation of such systems and networks."

The manual applies to all DIA, DoD (expanded, but, not including NSA) and DoD contractors using ADP systems to process SCI. Patently, this manual was not written to apply to systems processing collateral WNINTEL.

RESOURCE IMPACT:

A. Drafting Group:

Retention of the DCID's scope is, by far, the least costly approach; since we can proceed to other issues, once this question is answered. Changing the scope is likely to take considerable time with minimal payoff.

B. Intelligence Community:

Retention of the current scope appears to be "revenue neutral", in that it will not change the number of systems covered nor, from this decision only, their operating modes. However, it may well be that, if we properly clarify and promulgate what the current DCID says, there may be less confusion about the required protections. This could result in some change in costs. The magnitude of such a change and, perhaps, even its direction, are difficult to quantify.

RECOMMENDATION:

That the scope of the current DCID be retained, but, clarified, for the rewrite. Some clarifying sentences that should be added are: "Intelligence" includes sensitive compartmented information (SCI) as defined in DCID 1/19 and that information which currently is (or should be) marked "Warning Notice-Intelligence Sources or Methods Involved (WNINTEL)" as defined in DCID 1/7. This marking is used to identify classified intelligence whose sensitivity requires constraints on its further dissemination and use. This marking may be used only on intelligence which identifies or would reasonably permit identification of an intelligence source or method which is susceptible to countermeasures that could nullify or reduce its effectiveness. To avoid confusion as to the extent of dissemination and use restrictions governing the information involved, this marking may not be used in conjunction with special access or Sensitive Compartmented Information (SCI) controls. Additional clarification can be found in DCID 1/7.

DECISION:

AGREE WITH RECOMMENDATION that the scope of the current DCID be retained, but, clarified, for the rewrite.

DISAGREE WITH RECOMMENDATION. In other words, the scope of the current DCID must be modified for the rewrite.